IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PERSON OF CHAD LAWLOR, ONE 2010 VOLKSWAGEN JETTA, GREY IN COLOR, NH REGISTRATION DD2BHJS, AND ANY ELECTRONIC DEVICES FOUND IN EITHER LOCATION	Case No. 21-mj -93-01/03-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Adam Rayho, a Task Force Officer with the United States Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

1. I am a detective with the Nashua, New Hampshire Police Department, and a deputized task force officer (TFO) for HSI. I became a certified police officer in the State of New Hampshire in May 2014 after graduating from the 164th New Hampshire Police Standards and Training Academy. I have also completed HSI's Task Force Officer Course. I hold a bachelor's degree in criminal justice, with a minor in Computer Science and Victimology, from Endicott College. Since November 2019, I have been assigned to the Special Investigations Division as a member to the New Hampshire Internet Crimes Against Children (ICAC) Task Force, which includes numerous federal, state, and local law enforcement agencies conducting proactive and reactive investigations involving online child exploitation. As a TFO, I am authorized to investigate violations of federal laws and to execute warrants issued under the authority of the United States. Specifically, as a TFO and a member of the ICAC, I investigate

criminal violations related to online sexual exploitation of children. I have received training in the areas of child sexual exploitation including, but not limited to, possession, distribution, receipt, and production of child pornography, and interstate travel with intent to engage in criminal sexual activity, by attending training hosted by the ICAC involving online undercover chat investigations and interview/interrogation. I have also participated in numerous online trainings hosted by the Federal Bureau of Investigation Child Exploitation and Human Trafficking Task Force Online Covert Employee Development Series. These trainings focused on live stream investigations, using undercover personas on various social media applications for proactive investigations, including on Kik Messenger. In addition, I have completed the Cellebrite Certified Operator and Cellebrite Certified Physical Analyst course in mobile forensics. As part of my duties, I have observed and reviewed examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, to include digital/computer media. During the course of this investigation, I have also conferred with other investigators who specialize in computer forensics and who have conducted numerous investigations which involved child sexual exploitation offenses.

2. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant relating to Chad Lawlor (hereafter "LAWLOR") who is the target of an ongoing investigation into possession and distribution of child pornography, and who lives in Manchester, NH. This affidavit is submitted in support of a warrant to search (1) the person of Chad Lawlor and (2) any electronic devices and/or digital

storage media found on the person of Chad Lawlor. The search warrants, as described more fully below and in the respective Attachment B seek authority to search for and to seize electronic devices and electronic media found on the person of LAWLOR, for the things described in the respective Attachment B – specifically, evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B), the illegal possession and distribution of child pornography.

4. During the course of this investigation I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. § 2252(a)(4)(B) and 18 U.S.C. § 2252A(a)(2), related to the possession and distribution of child pornography in the District of New Hampshire. 18 U.S.C. § 2252(a)(4)(B) makes it a crime for any person to knowingly possess one or more images depicting a minor under the age of 18 engaged in sexually explicit conduct. 18 U.S.C. § 2252A(a)(2) makes it a crime for any person to knowingly receive or distribute any child pornography that has been mailed, or using any means

or facility of interstate or foreign commerce, or that has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

7. "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

8. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

9. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

10. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

11. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers).

12. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

13. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each

time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

PROBABLE CAUSE

14. Kik is a free application, or "app," that is primarily used on mobile or "smart" devices, such as an Apple iPhone, Android cell phone, Apple iPad, or Android tablet. Once downloaded onto a compatible device, Kik permits users to chat with other individuals one-on-one and in groups as well as share pictures and videos. Each user has the ability to create a screen name which can be changed at any time. The app allows the user to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content over the internet after the user registers a username. Although Kik is a platform for mobile devices, there are ways that it can be used on desktop or laptop computers. In order to do so, a person would have to install on the computer what is known as an "emulator," a program that emulates a mobile device environment.

15. Kik messenger allows individuals to create public or private groups on their server which allows for multiple individuals to communicate and share files. Individuals within the Kik group are also able to privately message other individuals within the group. The creator of the Kik group is called an owner. Through my training and experience, I know that the owner of a Kik group is either the individual who created the group or the longest active member if the original owner has left the group. The owner of the group can make members of the group administrators, which gives them the same privileges as the owner, such as adding individuals and removing them.

16. On February 01, 2021, while searching for groups on Kik messenger that are dedicated to the sexual exploitation of chidren, I observed a group titled NH D.aughters with the

unique username #nhdau.ghterfantasy. Through my training and experience I recognized this group name as one that could be associated with the exploitation of children. The current rank structure of the Kik group #nhdau.ghterfantasy lists the owner as "JJ" unique username " and administrator as "Jack Daniels" unique username ".

17. Using an undercover Kik account and the persona of an adult male with two minor children, I joined the group. Between February 01, 2021, and continuing through the beginning of April 2021, I have observed several conversations within the group and have had private conversations with members of the group which showed the majority of the members join or use the group to discuss the exploitation of children. One such example is Kik user " who has been identified as Kyle Amaral ("AMARAL") of Ossipee, New Hampshire. AMARAL joined the group on February 16, 2021 and was a member until February 20, 2021. AMARAL was identified by Detective J.B. Reid of the Boone North Carolina Police Department and North Carolina ICAC / Homeland Security Investigations as an individual producing child sexual abuse material involving his three-year-old daughter. During the time AMARAL was a member of the group, I observed him communicate with " in the group message setting. Based on conversations they had, it appeared they began to privately message each other.

18. In furtherance of the AMARAL investigation, I completed a search warrant for the Kik account " " which was signed into effect by United States Magistrate Judge Andrea Johnstone. The results from Kik/Media Lab showed that " sent files through the Kik chat platform to various Kik users, including . In total, twenty-four files were sent from " " to " ". Each file contained a unique ID created by Kik to identify the file along with the date, time, and IP address from which the file was sent. In

reviewing these files, I observed eight files which were sent from " to " which qualified as child sexual abuse material. Two of these eight images are described as:

Unique ID: 0021
Date/Time: 02-17-2021 at 13:25:23 UTC
Description: Digital image of a female toddler lying on her back with her onesie unzipped. The penis of an adult male is being inserted into the child's vaginal opening.

Unique ID: 2cd
Date/Time: 02-17-2021 at 16:04:21 UTC
Description: Digital image of a female toddler from the belly button down. The child's underwear is pulled to the side exposing her vaginal opening. There is a white liquid substance that appears to be ejaculate covering the child's vaginal opening.

19. KIK also provided files sent by other Kik users via the Kik chat platform to " including files sent by " . In total, eleven files were sent from " " to " " Each file contained a unique ID created by Kik to identify the file along with the date, and time the file was sent. Upon reviewing these files, I observed seven files which were sent from to " which qualified as child sexual abuse material. Two of these files are described as:

Unique ID: 9c0
Date/Time: 02-17-2021 at 13:26:15 UTC
Sent From: Gallery
Description: A series of two digital images involving prepubescent females. In the second image the prepubescent female has her shirt pulled up exposing her vaginal and anal openings. Additionally, there is a white liquid substance that appears to be ejaculate on the female's vaginal opening. In identifying the female as prepubescent, I base it off the female's bone structure and lack of pubic hair.

Unique ID: 9f5
Date/Time: 02-17-2021 at 16:25:30 UTC
Sent From: Gallery
Description: Thirty-four second video of a prepubescent female performing oral sex on an adult male. Approximately halfway through the video it transitions to the prepubescent female's vagina being penetrated by an adult male's penis. In identifying the female in the video as prepubescent, I base it off the female's bone structure, lack of pubic hair, and lack of breast development.

20. Starting on February 01, 2021, and continuing through April 2021, I spoke with Kik user " " using my undercover persona via the private message feature of Kik messenger. " " sent me a private message after I joined the NH D.aughters group asking for pictures of my daughters. During my conversations with " I provided him with an age-regressed image of a Nashua Police Department employee who I identified as my 12 year old daughter and an age-regressed image of a Nashua Police Department employee who I identified as my 10 year old daughter. " proceeded to ask for pictures of the individuals in their bathing suits or underwear and asked me to "sneak some pics in their undies". " " identified his children as 12 and 9 years old and spoke about "hooking up" with a 12 year old in the past whom he met on AOL in the early 2000's.

21. This conversation led into a conversation regarding my children being sexually active. I asked what he would like to do to them, to which responded, "maybe eat their pussies and finger them". " " brought up meeting me and my children, but requested I send a "live" picture of both the children in their "undies" prior to the meeting to prove I was not a cop.

22. Through my training and experience in the use of Kik messenger, I know a "live" picture means one taken from the Kik application which will display the word "camera" underneath. Comparatively, if a file is sent from the user's gallery it will not display "camera". During later conversations, asked me if I had "pics of other young girls" which clarified to mean "preteen and up". " also later requested "naked" pictures of my daughters. Lastly, during a conversation with " " on March 01, 2021, I brought up the Kik user " " (this is the same user that is associated with the "

Kik display name). I advised I had previously traded pictures with Jon Claw and " replied, "He (Jon Claw) sent me some sexy pics of his daughters".

23. On February 25, 2021 Detective J.B. Reid provided me with private message Kik chats between his UC profile, which is that of an adult female, and . Detective Reid and " were both members of another Kik group which AMARAL was formerly the owner of. Of investigative interest is a conversation from February 25, 2021 between 12:41 P.M. and 1:37 P.M., in which sends a "live" selfie style picture of himself. Comparing this image to arrest photos of Chad Lawlor, I was later able to positively identify this individual as Lawlor. Furthermore, at 1:34 P.M., sends IMG_0299.mp4 which is a fifty-three second video of a female child wearing a shirt with her pants pulled down. The female is dancing for the camera and eventually turns her body so her buttocks is the focal point of the video. As the video continues the female makes her vaginal opening the focal point of the video and begins to insert her fingers into her vaginal opening.

24. On March 10, 2021, I received an email from Kik/MediaLab containing the results of an HSI summons for subscriber information related to the Kik user " . Upon viewing the subscriber information, I observed the following items of investigative interest:

First Name: Jack
Last Name: Daniels
Email: @yahoo.com (confirmed)
Username:
Device Information: Samsung (Model SM-A716U)
Birthday: 1975

25. Included with the subscriber information, Kik/MediaLab also provided 6,667 IP addresses used by " to access the Kik chat network from February 08, 2021 to

March 10, 2021. Reviewing these IP addresses, I observed 1,277 which were associated with "WIFI" networks and 5,390 which were associated with "MOBILE" networks. Through my training and experience, I know that "WIFI" is a wireless network technology that allows a subscriber of internet services (provided through an internet service provider such as Comcast, Fairpoint Communications, etc.) to access the internet on computers and other internet capable devices within a fixed location without a physically wired internet connection. In contrast, connecting to the internet via a "MOBILE" network means that the individual is using the cellular data network associated with his/her mobile service provider, e.g. Verizon, AT&T, T-Mobile, etc., to access the internet. In reviewing the IP addresses provided by Kik/MediaLab, " primarily uses a "MOBILE" network to access the Kik chat network. This, coupled with the fact that Kik is primarily a mobile application, appears to indicate that the target is using the Kik application and Kik chat network primarily, if not exclusively, on a mobile device such as a cell phone or tablet.

26. In further analyzing the IP addresses provided by Kik/MediaLab, I identified a residential IP address, 73.60.51.70, which was used by " to access the Kik chat network approximately 600 times during the relevant one-month time period. On March 17, 2021, a summons was issued to Comcast Cable Communications for subscriber information associated with this IP address. The return from Comcast showed that during the relevant timeframe, the subscriber for IP Address 73.60.51.70 was:

Subscriber Name: Loreann Lacasse

Service Address: *Manchester, New Hampshire 03102*

I subsequently identified Loreann Lacasse as Chad LAWLOR'S ex-wife.

27. On March 29, 2021, I made contact with Officer Konrad Jaworowski of the Manchester Police Department ("MPD") Sex Offender Registration/Compliance Unit in regards to Chad LAWLOR. Due to a 2005 Massachusetts conviction for sexual assault, LAWLOR is Tier II Registered Sex Offender in New Hampshire and must register semi-annually for life. Officer Jaworowski provided me LAWLOR'S most recent sex offender registration form, which was completed on February 09, 2021. On the form, LAWLOR lists his address as Manchester, New Hampshire.

28. Using the photo provided by Detective J.B. Reid of Kik user ", I conducted research on Facebook and observed a Facebook profile picture for Chad LAWLOR (DOB: 1975) (https://www.). The profile picture for LAWLOR'S Facebook account appears to depict the same person depicted in the picture sent by Kik user " " to Detective Reid. LAWLOR'S Facebook profile also includes pictures of three minor children (one male and two females).

29. A query of the New Hampshire Department of Motor Vehicles database shows one vehicle registered to LAWLOR: a 2010 Volkswagen Jetta, grey in color, NH registration The vehicle's registration expired in August 2020, however I observed this vehicle parked in front of the Douglas Street address on Friday, April 2, 2021, and at LAWLOR'S place of employment on April 5th and 6th, 2021. Based on these observations, it appears that LAWLOR continues to drive this vehicle despite the registration being expired.

30. I am aware, through my training and experience, that individuals who collect and traffic in child pornography often maintain their collections over long periods of time and take measures to safeguard their collections and to avoid detection. I am also aware that electronic devices such as cell phones are by their very nature portable and often contain a

wealth of highly personal and confidential information that individuals have an interest in safeguarding. For this reason, individuals often keep their personal electronic devices such as cell phones on or near their person at all times, or in their home or vehicle.

BIOMETRIC ACCESS TO DEVICES

31. This warrant seeks authorization for law enforcement to compel LAWLOR to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. Grounds for this request follow.

32. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

33. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

34. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front- facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

35. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

36. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

37. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the

DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

38. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

39. In light of the foregoing, and with respect to any device found on LAWLOR'S person, law enforcement personnel seek authorization, during execution of this search warrant, to: (1) press or swipe the fingers (including thumbs) of LAWLOR to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of LAWLOR and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of LAWLOR and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

40. The proposed warrant does not authorize law enforcement to compel LAWLOR to state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel LAWLOR to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

41. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crime of possessing and distributing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and 2252A(a)(2) may be located on LAWLOR'S person, and, in particular, within any electronic devices found on LAWLOR'S person. I therefore seek a warrant to search LAWLOR'S person and any electronic device and/or storage media found on his person, and to seize the items described in Attachment B.

42. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the search of LAWLOR'S person and/or vehicle. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

/s/ Adam Rayho
Adam Rayho
Task Force Officer
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Apr 6, 2021

Time: 3:23 PM, Apr 6, 2021

Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire